The place where breaking news, BitTorrent and copyright collide

Which VPN Providers Really Take Anonymity Seriously?

enigmax

October 7, 2011

322

Anonymity, privacy, vpn

Print

Last month it became apparent that not all VPN providers live up to their marketing after an alleged member of Lulzsec was tracked down after using a supposedly anonymous service from HideMyAss. We wanted to know which VPN providers take privacy extremely seriously so we asked many of the leading providers two very straightforward questions. Their responses will be of interest to anyone concerned with anonymity issues.

As detailed in yesterday's article, if a VPN provider carries logs of their users' activities the chances of them not being able to live up to their claim of offering an anonymous service begins to decrease rapidly.

There are dozens of VPN providers, many of which carry marketing on their web pages which suggests that the anonymity of their subscribers is a top priority. But is it really? Do their privacy policies stand up to scrutiny? We decided to find out.

Over the past two weeks TorrentFreak contacted some of the leading, most-advertised, and most talked about VPN providers in the file-sharing and anonymity space. Rather than trying to decipher what their often-confusing marketing lingo really means, we asked them two direct questions instead:

1. Do you keep ANY logs which would allow you or a 3rd party to match an IP address and a time stamp to a user of your service? If so, exactly what information do you hold?

2. Under what jurisdictions does your company operate and under what exact circumstances will you share the information you hold with a 3rd party?

This article does not attempt to consider the actual quality of service offered by any listed provider, nor does it consider whether any service is good value for money. All we are interested in is this: Do they live up to claims that they provide a 100% anonymous service? So here we go, VPN providers in the file-sharing space first.

VPN providers marketed strongly in the P2P space

BTguard

Response to Q1: “It’s technically unfeasible for us to maintain log files with the amount of connections we route,” BTguard explain. “We estimate the capacity needed to store log files would be 4TB per day.”

Response to Q2: “The jurisdiction is Canada. Since we do not have log files, we have no information to share. We do not communicate with any third parties. The only event we would even communicate with a third party is if we received a court order. We would then be forced to notify them we have no information. This has not happened yet.”

BTguard website

ItsHidden

Response to Q1: “No logs, they are not kept. Even system logs that do not directly link to users are rotated on an hourly basis.”

Response to Q2: “The company has recently been sold and falls under the Jurisdiction of the Seychelles. As such there is no requirement [to log] within that jurisdiction.”

ItsHidden website

TorrentPrivacy

Response to Q1: “We have connection logs, but we don’t store IP addresses there. These logs are kept for 7 days. Though it’s impossible to determine who exactly have used the service.”

Response to Q2: “We have servers in Netherlands, Sweden and USA while our company is based on Seychelles. We do not disclose any information to 3rd parties and this can be done only in case of a certain lawsuit filed against our company.”

TorrentPrivacy website

Ipredator

Response to Q1: “We don’t store the IP at all actually. It’s in temporary use for the session you have when you’re connected but that’s it. We’ve had very few issues with not having logs, but not keeping them makes it safer even for us since we can’t accidentally give out information about anyone.”

Response to Q2: “We fall – mostly – under Swedish jurisdiction when it comes to the service. When it comes to organisational stuff (who keeps the data, who owns the service, who owns the server, who owns the network etc etc) it’s very mixed, intentionally. This is to make it hard and/or impossible to legally bully us around if that would be the case.”

“We can’t be easily shut down, and we can’t be pressured by courts to implement stuff

we would oppose. For end-users this is not affecting them in a negative way at all, only the opposite."

Ipredator website

Faceless

Response to Q1: "We do not log any IP addresses and no information about what data is accessed by our users, so we have no information that could be interesting to third-parties."

Response to Q2: "We have servers in The Netherlands and our company is based in Cyprus. If authorities would contact us we would have to tell them that we have no connection logs or IP-addresses saved on our systems."

Faceless website

General VPN providers

AirVPN

Response to Q1: The company carries no identifying logs.

Response to Q2: "Jurisdiction is in the EU, under most circumstances Italy (country of the company and home of the person legally responsible for data protection), but applicable law may be one of the EU Member States where the servers of the network are physically located (no servers are in Italy)," AirVPN told us.

"We don't share any information with anyone."

AirVPN website

VPNReactor

Response to Q1: "Only for 5 days to stop abuse[..]. After 5 days we have absolutely no way to match any IP address or time stamp to any users. Privacy and Security is further enhanced for individual users because their VPN connections are basically lost in the crowd."

"Our free VPN users share a block of IPs when they connect to the internet via VPNReactor. So at any given time hundreds/thousands of our VPN users that have active connections could all be sharing a single IP address. None of our VPN users are assigned individual public IPs."

Response to Q2: "We strive to be upfront and transparent with our logging policies for the benefit of our VPN users." Logs seen by TorrentFreak seemed to confirm no identifiable information being stored.

"We are a U.S. based company and are bound by U.S. based court orders,"

VPNReactor continued. “However, if a U.S. based subpoena comes in requesting info for activity that occurred more then 5 days prior, we have absolutely nothing to provide as our logs would have expired off. Request for connection details outside a U.S. based court order will be fully ignored.”

VPNReactor website

BlackVPN

Response to Q1: “We do not keep any logs about our users internet activities including which sites they access or what data they transfer. We also run log cleaners on our systems which removes the IPs from logs before they are written to disk,” the company told TorrentFreak.

“For tax and legal reasons we do store some billing information (name, email, country), but it is stored with a third-party and separate from the rest of BlackVPN.”

BlackVPN say they hold a username and email address of their subscribers and the times of connection and disconnection to their services along with bandwidth consumption. Logging is carried out as follows:

“On our Privacy Servers, NL & LT we don’t log anything that can identify the user, but on our US & UK server where we don’t allow sharing copyrighted materials we do log the internal RFC1918 IP that is assigned to the user at a specific time,” BlackVPN explain.

“So to clarify, we don’t log the real external IP of the user, just our RFC1918 internal one, this we have to do to comply with local laws and to be able to handle DMCAs.”

Response to Q2: “We operate under the jurisdiction of the Netherlands and we will fiercely protect the privacy and rights of our users and we will not disclose any information on our users to anyone, unless forced to by law enforcement personnel that have produced the proper legal compliance documents or a court order. (In which case we don’t really have a choice).”

BlackVPN website

PrivatVPN

Response to Q1: “We don’t keep ANY logs that allow us or a 3rd party to match an IP address and a time stamp to a user our service. The only thing we log are e-mails and usernames but it’s not possible to bind a activity on the Internet to a user.”

Please note: PrivatVPN also offer use of a US server for watching services like Hulu. IP logs are kept when users use this service.

Response to Q2: “Since we do not log any IP addresses [we have] nothing to disclose. Circumstances doesn’t matter in this case, we have no information regarding our customers’ IP addresses.”

PrivatVPN website

Privacy.io

Response to Q1: “No logs whatsoever are kept. We therefore simply are not able to hand data out. We believe that if you are not required to have logs, then you shouldn’t. It can only cause issues as seen with the many data leaks in recent years. Should legislation change in the juristictions we operate in, then we’ll move. And if that’s not possible, then we’ll shut the service down. No compromises.”

Response to Q2: “We span several jurisdictions to make our service less prone for legal attacks. Servers are currently located in Sweden. We do not share data because we don’t have it. We built this system because we believe only when communicating anonymously, you can really freely express yourself. As soon as you make a compromise, you are going down a slippery slope to surveilance. People will ask for more and more data retention as seen around the world in many countries recently. We do it because we believe in this, and not for the money.”

Privacy.io website

Mullvad

Response to Q1: “No. And we don’t see why anyone would. It would be dishonest towards our customers and mean *more* potential legal trouble.”

Response to Q2: “Swedish jurisdiction. We don’t know of any way in which the Swedish state in practice could make us behave badly towards our clients and that has never happened. Another sign we take privacy seriously is that we accept payments in Bitcoin and cash in the mail.”

Mullvad website

Cryptocloud

Response to Q1: “We log nothing at all.”

Response to Q2: “We don’t log anything on the customer usage side so there are no dots to connect period, we completely separate the payment information,” they told us.

“Realistically unless you operate out of one of the ‘Axis of Evil Countries” Law Enforcement will find a way to put the screws to you,” Cryptocloud add.

“I have read the nonsense that being in Europe will protect you from US Law Enforcement, worked well for HMA didn’t it? Furthermore I am pretty sure the Swiss Banking veil was penetrated and historically that is more defend-able than individual privacy. The way to solve this is just not to log, period.”

Cryptocloud website

VPN providers who log, sometimes a lot

VyprVPN

VyprVPN is the VPN service connected to and offered by the Giganews Usenet service, although it can be used completely standalone. In common with many other providers we contacted, VyprVPN acknowledged receipt of our questions but then failed to respond. We've included them here since they have such a high-profile.

The company policy says that logging data "is maintained for use with billing, troubleshooting, service offering evaluation, [Terms of Service] issues, [Acceptable Use Policy] issues, and for handling crimes performed over the service. We maintain this level of information on a per-session basis for at least 90 days."

On Usenet forum NZBMatrix several users have reported having their VyprVPN service terminated after the company processed "a backlog" of DMCA notices which pushed them over the "two-strikes-and-out" acceptable use policy.

So, does VyprVPN log? You bet.

SwissVPN

We included SwissVPN in our survey because they are well known, relatively cheap and have been used by those on a tight budget. To their credit, they were also the fastest company to respond. They are one of the few companies that do not make anonymity claims.

Response to Q1: "SwissVPN is being operated based on Swiss Telecommunications and Personal Data Protection Law. Session IP's (not visited content, websites, mail, etc.) are being logged for 6 months," the company told us.

Response to Q2: The company responds to requests from 3rd parties under Swiss criminal law (pdf).

SwissVPN website

StrongVPN

This company did not directly answer our questions but pointed us to their logkeeping policy instead.

StrongVPN do log and are able to match an external IP address to their subscribers. We have included them here since they were the most outwardly aggressive provider in our survey when it came to dealing with infringement.

"StrongVPN does not restrict P2P usage, but please note sharing of Copyrighted materials is forbidden, please do not do this or we will have to take action against your account," they told us, later adding in a separate mail: "StrongVPN Notice: You may NOT distribute copyright-protected material through our network. We may cancel your account if that happens."

StrongVPN website

Disappointing: VPN providers who simply failed to respond

In addition to the above, TorrentFreak also approached a number of other fairly well known VPN providers. It's not clear if our questions were simply too tricky to answer in a positive light or whether there was some other reason, but disappointingly none of them responded to our emails, despite in some cases having acknowledged receipt of our questions.

They include Blacklogic.com, PureVPN.com, VPNTunnel.se [Update: VPNTunnel.se have now responded, see here], Bolehvpn.net [Update: Boleh responded after publication - they carry no logs] and Ivacy.com.

Should the above now feel able to respond directly to our questions, or if there are any other VPN providers reading who would like to be included in a future update, please contact us now with direct responses to the questions above. Apologies to the providers who contacted us at the last minute but were too late to be included in the report – we had to stop somewhere.

Final thoughts

When signing up to a VPN provider it really is evident that their their logging and privacy policies should be read slowly. And then read again, even more slowly than at first. Many are not as straightforward as they first appear (some even seem to be deliberately misleading) and that is the very reason why we asked our own questions instead.

In contrast to the the pessimism generated by yesterday's report, as we can see from the list above, when it comes to offering real privacy there are plenty of services out there.